EFFICIENT BINARY EXTENDED ALGORITHM USING SGN FUNCTION

Anton Iliev, Nikolay Kyurkchiev,
Asen Rahnev, Todorka Terzieva

Abstract. *We present new binary extended algorithms, which work for every integer numbers a and b for which* $a \neq 0$ *and* $b \neq 0$*. The approach given here generalizes and optimizes the algorithm given in the monograph of A. Menezes, P. Oorschot and S. Vanstone [3] as well our results from [2] and [1]. These computation ways demonstrate high computational effectiveness especially for long numbers.*

Acknowledgments

This work has been accomplished with the financial support by the Grant No BG05M2OP001-1.001-0003, financed by the Science and Education for Smart Growth Operational Program (2014-2020) and co-financed by the European Union through the European structural and Investment funds.

References

[1] A. Iliev, N. Kyurkchiev, A. Rahnev, Recursive Extended Stein's Binary Algorithm, *International Electronic Journal of Pure and Applied Mathematics*, (2021), **14**, No. 1, 31–36.

[2] A. Iliev, N. Kyurkchiev, A. Rahnev, A New Improvement of Extended Stein's Binary Algorithm, *Proceedings of the Anniversary International Scientific Conference "Synergetics and Reflection in Mathematics Education"*, Pamporovo, 16–18 October 2020, Plovdiv University Press, (2020), 259–264.

[3] A. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, 5th ed., CRC Press LLC, New York, (2001).

Anton Iliev[1,2,*], Nikolay Kyurkchiev[1,2], Asen Rahnev[1], Todorka Terzieva[1]
[1] Faculty of Mathematics and Informatics,
Paisii Hilendarski University of Plovdiv,

24, Tzar Asen Str., 4000 Plovdiv, Bulgaria,
[2] Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl. 8, 1113 Sofia, Bulgaria
Emails: nkyurk@uni-plovdiv.bg, assen@uni-plovdiv.bg,
dora@uni-plovdiv.bg, aiiliev@math.bas.bg, nkyurk@math.bas.bg
[*] Corresponding author: aii@uni-plovdiv.bg